

Middle East and North Africa

FEBRUARY 2026

Introduction

Cybersecurity risk in 2026 is accelerating, fuelled by advances in AI, deepening geopolitical fragmentation and the complexity of supply chains. This analysis builds on the *Global Cybersecurity Outlook 2026* (GCO 2026) to examine how these global trends are playing out in the Middle East and North Africa, providing a focused view of the region's evolving cybersecurity landscape.¹

Key takeaways on Middle East and North Africa

- 93% of organizations in the region believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months. This compares to the global perception at 94%.
- 77% of businesses in the Middle East and North Africa already implemented AI enabled tools to fulfil their cybersecurity objectives, in line with the global average.
- 85% of organizations express confidence in national capabilities to respond to cyber incidents targeting critical infrastructure – the highest across all regions (globally 37%).
- Respondents in the Middle East and North Africa are showing the strongest confidence in their organizations' cyber resilience compared to the other regions with 40% of organizations in this region rating their cyber resilience as exceeding requirements (globally 19%).
- To mitigate supply chain risks, 73% of organizations in this region prioritise assessing their supplier security maturity, while 67% involved their security function in the procurement process
- 47% of businesses in the Middle East and North Africa report they lack the workforce skills required to meet their current cybersecurity objectives. This is just below the global average (49%).

AI security

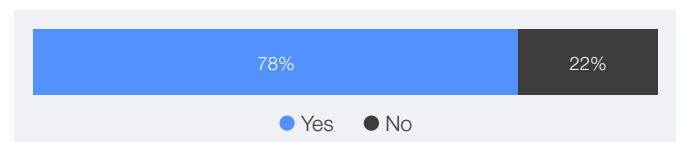
AI risk perception

- According to the GCO 2026 survey, 93% of organizations in the region believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months and 82% report that AI-related risks have increased (globally 94% and 87% respectively).
- Furthermore, data leaks and advancement of adversarial capabilities are considered the most pressing cybersecurity issues linked to generative AI in this region, cited by 31% of respondents.
- This heightened concern is not unique to the Middle East and North Africa, but the region appears better prepared compared to other regions. Some 69% of organizations report that they assess the security of AI tools at least once or periodically before deployment (globally 64%).

AI for security

- Organizations in the Middle East and North Africa are actively adopting AI-enabled tools to strengthen their cybersecurity posture, with the survey indicating that 78% have already implemented such solutions, signalling strong momentum towards AI-driven security even if barriers remain.

Has your organization implemented any AI-enabled tools to fulfil its cybersecurity objectives?



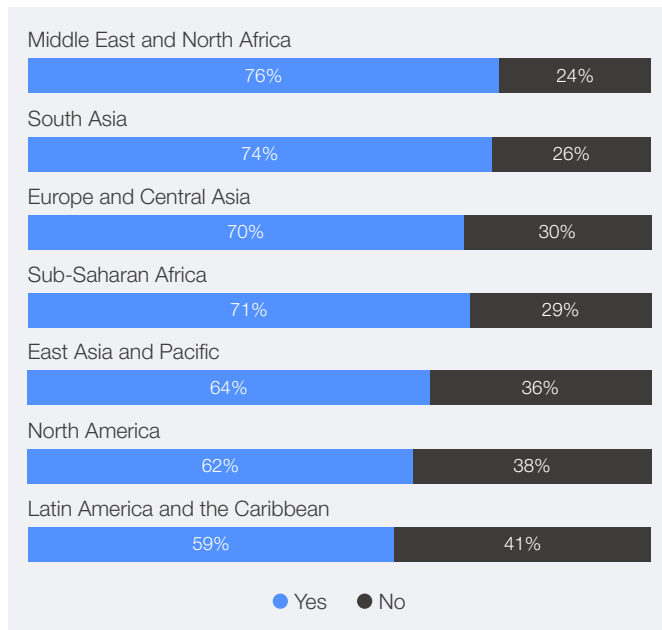
- Despite this progress, organizations in the region report the following as key hurdles in adopting AI for cybersecurity:
 1. Insufficient skills (58%)
 2. Human validation required for AI-generated security responses (47%)

¹ The number of respondents from this region in the GCO 2026 survey is lower than in other regions. As a result, the findings may have reduced statistical robustness and should be interpreted with due caution.

Geopolitics

- 76% of organizations in the Middle East and North Africa report adjusting their cybersecurity strategies due to geopolitical volatility – which is higher than all other regions (globally 66%). Additionally, 69% report incorporating geopolitically motivated cyberattacks into risk mitigation plans – the highest proportion among other regions (globally 64%).

Has your organization's cybersecurity strategy evolved because of geopolitical volatility?



- The Middle East and North Africa region shows by far the highest trust in national capabilities to respond to cyber incidents targeting critical infrastructure, with nearly 84% of organizations expressing confidence (globally 37%).

Cybercrime

- The GCO 2026 survey reveals that exploitation of software vulnerabilities and ransomware attacks are the top two perceived cyber risks in the region.

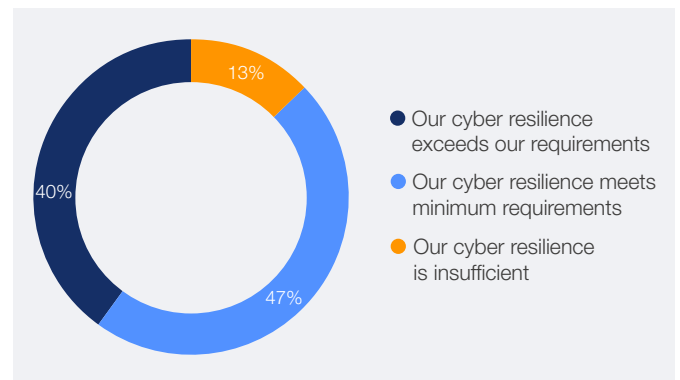
Rank	Which cyber risks concern you most for your organization?
1	Exploitation of software vulnerabilities
2	Ransomware attack
3	Supply chain disruption

- 62% of respondents from the Middle East and North Africa report that they or someone in their professional/personal network has been affected by cyber-enabled fraud in the past 12 months (globally 73%). Nearly 50% indicate that these were phishing, vishing or smishing attacks.

Resilience

- The Middle East and North Africa region is showing the strongest confidence in cyber resilience compared to other regions:
 - 40% of organizations in the region rated their cyber resilience as exceeding requirements ((globally 19%)
 - 47% assessed their cyber resilience as meeting minium requirements (globally 64%)
 - 13% assessed it as insufficient (17% globally)
- The top three challenges to achieving cyber resilience in this region are:
 1. Rapidly evolving threat landscape and emerging technologies (64%)
 2. Cybersecurity skills and expertise shortage (58%)
 3. Third-party and supply chain vulnerabilities (56%)

How would you rate your organization's cyber resilience?



Supply chain

- The top three cyber risks related to supply chain security reported by organizations in the region are:
 1. Visibility: Lack of visibility into their own organization's extended supply chain
 2. Inheritance risk: Inability to assure integrity of third-party software, hardware and services
 3. Concentration risk: A high degree of dependence on critical third-party suppliers
- To mitigate these risks, 73% of organizations in the region prioritize assessing their supplier security maturity, while 67% involve their security function in the procurement process.

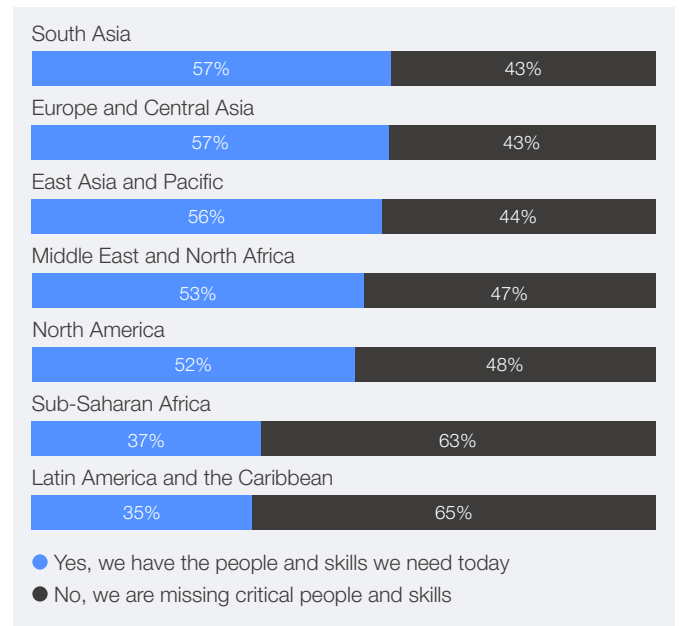
How does your organization address supply chain cyber risk?



Cyber skills

- 53% of organizations in the Middle East and North Africa report having the necessary people and skills to meet cybersecurity objectives (globally 50%).
- However, 58% of organizations in the region identify shortages in cybersecurity skills and expertise as one of the biggest obstacles to becoming cyber-resilient (45% globally).

Does your organization's workforce have the skills needed to achieve its current cybersecurity objectives?



*Some graphs may show percentages exceeding 100% due to multiple-choice questions and rounding.

To read the full report [Global Cybersecurity Outlook 2026](#) on cybersecurity risks and trends at a global scale, please visit wef.ch/cybersecurity26. Explore the data deeper with our accompanying [Data Explorer](#).